

Research and Implementation of FM-DCSK Chaotic Communication System Based on GNU Radio Platform

Bingyan He, Yuanhui Yu and Lizhen Chen

Abstract FM-DCSK is a non-coherent modulation and demodulation technique, the output of which has the inherent wide-frequency performance will cause the estimation interference and the bit error rate decline. This paper designs and implements Frequency-modulated Differential Chaotic Shift Keying (FM-DCSK) Communication system based on GNU Radio platform. In order to get FM-DCSK signal, it needs to combine the FM modulation with the DCSK system. The bit energy of signals remained stable by using FM modulation so that the BER performance in such system can be improved. Since the system is based on software defined radio (SDR) to perform in a real-time wireless transmission, the bitrate, bandwidth and central frequency can be modified at ease. The experimental performance are discussed and compared to the theoretical performance.

Keywords Frequency-modulated differential chaotic shift keying · Chaos · Random-like property · Soft defined radio

1 Introduction

The unique initial value sensitivity, random-like property and unpredictability of chaotic signal can provide the guarantee for the secure transmission of information. The basic idea of chaotic secure communication is that using chaotic signal as a carrier, the transmitting data signal is hidden in the chaotic carrier, the waveform of the modulated chaotic signal is disorderly and irregular, not easy to be stolen. Chaotic signal is seemingly unpredictable, in fact, it is pseudo random signal which can be described using mathematical equations describing the broadband

B. He · Y. Yu · L. Chen (✉)
Computer Engineering College, JiMei University, Xiamen, China
e-mail: lzchen@jmu.edu.cn

B. He
e-mail: iceorspring@sina.com

characteristics make it widely used in the fields of multiple access communication and spread spectrum communication, etc.

Chaotic signals are a relatively new field of in communication systems. Potential of this method derived from the advantages offered by chaotic signals, such as robustness in multipath environments and resistance to jamming. Chaotic signals are non-periodic, broadband, and difficult to predict and reconstruct. These are properties which match with requirements for signals used in spread spectrum communication systems [1].

Various types of modulation can be used in direct chaotic communication systems like chaotic on-off keying (COOK). Differential chaotic shift keying (DCSK) and additive chaos modulation (ACM), etc. In all chaotic modulation types, DCSK with orthonormal basis properties offer the best robustness against the multipath and channel imperfections [2].

The performance of chaos-based digital communication systems under additive white Gaussian noise (AWGN) and m-distributed fading channels has been thoroughly studied [3, 4, 5].

SDR (Soft defined radio) is an intelligent wireless communication system, which can automatically sense the wireless environment and the use of spectrum. It's architecture has broken the traditional design pattern based on the special hardware, as much as possible using general hardware as the basic platform, to achieve wireless and communication functions by the software on the general processor, in order to achieve the wireless communication system upgraded and reconfigurable.

In this paper, we implement a FM-DCSK communication system on SDR. We put forward a simple and robust method to implement a Chaotic generator where the period loop length is sufficiently long and exactly known making this generator suitable for real-time transmissions. Considering complex wireless transmission environment, we study The symbol synchronization problem, and a better algorithm is proposed and implemented to make this system operational in real-time transmissions.

2 FM-DCSK Communication Scheme

A block diagram of FM-DCSK communication system is shown in Fig. 1 in this paper, This system uses FM-DCSK as a chaotic carrier to spread the digital signal over a wide frequency band. And modulate the digital signal to achieve the purpose of transmitting information. Firstly, the chaotic signal is generated by Logistic map, then Logistic signal is fed into the FM modulator, and FM-modulated Logistic signal is used as a new carrier. At the receiving end, the self correlation and cross-correlation of the chaotic signal are used to demodulation, and the digital sequence is obtained.

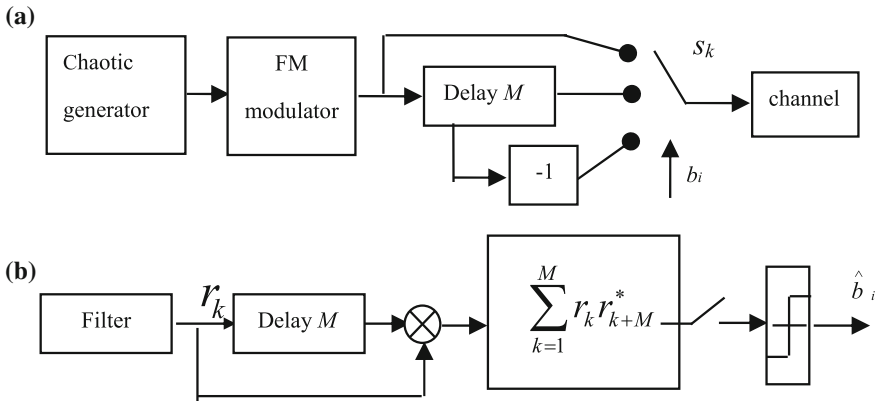


Fig. 1 a FM-DCSK transmitter b DCSK receiver

2.1 Generation of Chaotic Signal

Various types of chaotic and hyper-chaotic signals which are generated by various types of nonlinear circuits and are suitable for security communication are the hot topics in the field of physics and information science. Chaotic signal in this paper, we use Logistic mapping method to generate chaotic signal. At present, many research achievements have been made, such as Four order variant chaotic circuit, multi-scroll chaotic and super-chaotic circuit [6].

Considering the simplicity and good statistical properties of the logistic [7], the implementation of chaotic signal generator is based on the improved logistic full mapping equation, one-dimensional differential mapping equation is defined as follows:

$$X_{n+1} = 1 - X_n^2 \quad X_n \in (-1, 1) \tag{1}$$

X_0 is the initial value

$$E[X_n] = \lim_{M \rightarrow \infty} \frac{1}{M} \sum_{M=0}^{M-1} X_n = \int_{-1}^1 xf(x)dx = 0 \tag{2}$$

the X_0 has a very small change. After a certain number of iterative computations, it will produce completely different two sequences, making use of this feature, by setting the initial value, can generate a number of unrelated sequences. The DCSK system is not relevant and does not need to generate chaotic signals at the receiving side. In view of this, we use the Linux random number generator as the basic uniform random number generator. Linux random number generator produces random bytes from the entropy pool collected from the host computer activities such as the time

interval The user uses the keyboard, the distance and interval the mouse moves and the time interval between the specific interrupts, these host activities for the computer are nondeterministic and unpredictable. The kernel maintains an entropy pool based on these non deterministic device events, and the data in the pool are completely random. When there is a new device event coming, the kernel will estimate the randomness of the newly added data, when we get the data from the entropy pool, the kernel can reduce the estimated value of the entropy. Through the `get_random_bytes()` interface of the kernel, we can obtain the kernel 32 random integers from the entropy pool. Random integer range in $[-2^{31}, 2^{31} - 1]$, these random integers can be converted into $[-1, 1]$ range of floating point number.

The parabola map contains the basic idea of the modern chaos theory, including the basic frame and the model of the nonlinear theory, such as the period to chaos and bifurcation diagram. Then, by using the $F^{-1}(x)$ function to process the values of these uniform distributions, we obtain the random values of the Logistic distribution.

2.2 Modulation and Demodulation of FM-DCSK Signal

In the FM-DCSK [8] modulating system, the system firstly modulate the chaotic signal using FM modulation, and then the FM-modulated chaotic signal is used as the carrier for digital modulation. Since the energy of periodic positive cosine signal is constant in one cycle. So if the bit cycle is several times the cycle of positive cosine signal, you can ensure that the energy of each bit after the modulation of the FM-DCSK is not randomly variable. To realize the above description, as long as the frequency of positive cosine signal used to modulate chaotic signal is much higher than the chaotic signal, it can be easily achieved.

Firstly introducing Binary DCSK modulation, the modulated transmission signal can be expressed as

$$s_k = \begin{cases} c_k & 1 < k \leq M \\ b_i c_{k-M} & M < k \leq 2M \end{cases} \quad (3)$$

c_k is a chaotic reference signal, c_k has M chaotic signal samples, $2M$ is the number of chaotic samples sent per bit, M is an integer. A chaotic signal c_k as a reference signal is transmitted in the first half cycle of each bit, the data is transmitted in the second half of the cycle, if the data is 1, still transmitted chaotic signal c_k , if the data is 0, an inverted version of the chaotic signal to be transmitted.

Moreover, at the receiver side, the signal is embedded in an additive white complex Gaussian noise (AWGN) n_k with two side power spectral density equal to $2N_0$. Finally, the received signal is modeled as: $r_k = s_k + n_k$.

At the receiving side, the received quadrature signal r_k delayed by half a bit duration and correlated with undelayed signal. It then passes by a correlator where the reference and corresponding data samples are correlated. At last the sign of the

correlator output is computed to estimate the transmitted bit. In a practical implementation, many parameters like synchronization and time sampling correction must be taken into account to correctly achieve demodulation.

The output of the correlator is y_i .

$$\begin{aligned}
 y_i &= \sum_{k=1}^M r_k r_{K+M}^* = \sum_{k=1}^M [s_k + n_k][s_{k+M} + n_{k+M}]^* \\
 &= \sum_{K=1}^M [c_k + n_k][b_i c_{k+M} + n_{k+M}]^* \\
 &= b_i \sum_{K=1}^M c_k c_k^* + \sum_{K=1}^M c_k n_{k+M}^* + b_i \sum_{K=1}^M c_k^* n_k + \sum_{K=1}^M n_k n_{k+M}^*
 \end{aligned}
 \tag{4}$$

The first item is a useful signal and the second one is a random noise with zero mean value. It can be seen that the polarity of b_i and y_i is consistent, so the original signal can be demodulated. The decision threshold is 0, y_i is positive, then the data is 1, y_i is negative, the data is 0.

3 FM-DCSK Communication System Based on GNU Radio

GNU Radio [9] is a open and free software radio platform which can run on the common PC. It provides signal processing components to implement SDRs, through combining with the Minimal configuration hardware (mainly USRP), it can define the radio waves transmitting and receiving mode, and construct various wireless communication systems. It uses the two stage design, that data and control channel is separated. C++ is used to describe a variety of signal processing modules, Python is used for the configuration and connection between modules.

Figure 2 shows The whole FM-DCSK communication system model. In the GNU Radio platform, the parameter of the channel_model in the FM-DCSK communication system is as follows:

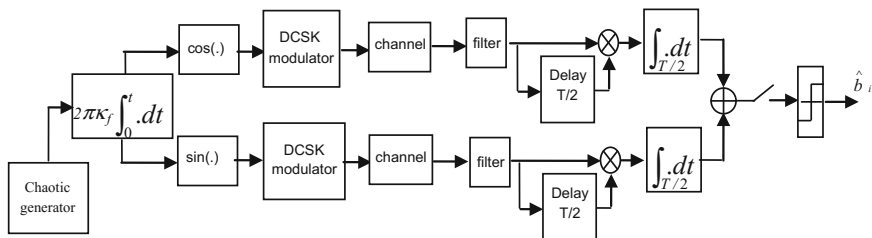


Fig. 2 The FM-DCSK system model

```
noise_voltage = 0.5; frequency_offset = 1e2/samp_rate; epsilon = 1.0;
taps = (1.0 + 1.0j); noise_seed = 0; samp_rate = 100 k.
```

In the GNU Radio platform, we design and encapsulate several blocks such as logistic Filter, Chaos Generator, Chaos Modulator and Chaos Demodulator, install these blocks to the GNU Radio platform. We can use these blocks to expand our chaotic communication system. The core function of the blocks is implemented by C++. The output of Chaos Generator is 32 bit float number. Chaos Modulator block implement a FM-DCSK modulation, this block has two inputs, one output and a parameter N_{samples} . One input is Frequency-modulated chaos, another input is data bit, the Frequency-modulated chaos is complex, the data is unsigned char.

Chaos Demodulator implement a demodulation of a chaotic signal, The input of this block is complex signal samples. The output is the value of the best synchronized correlation value. This block also includes a symbol synchronization algorithm in order to correct the phase and frequency errors of the radios. Figure 3 demonstrates the output wave of the Chaotic generator. Figure 4 shows the output wave of the Chaos Modulator.

The main problem of the DCSK receiving module is the symbol synchronization. Considering the USRP2 clocks are not synchronized and not controlled by software method, there are non-negligible drifts between the transmitter and the receiver clocks. This drift has a direct effect on the center frequency and the sampling rate. As the reference and data signals will be equally shifted in frequency, a small portion of noise will be mixed with the useful signal, resulting in a performance degradation. The sampling rate error is a bigger issue. Our synchronization algorithm tries to esynchronize symbols by finding the best auto-correlation value amongst multiple

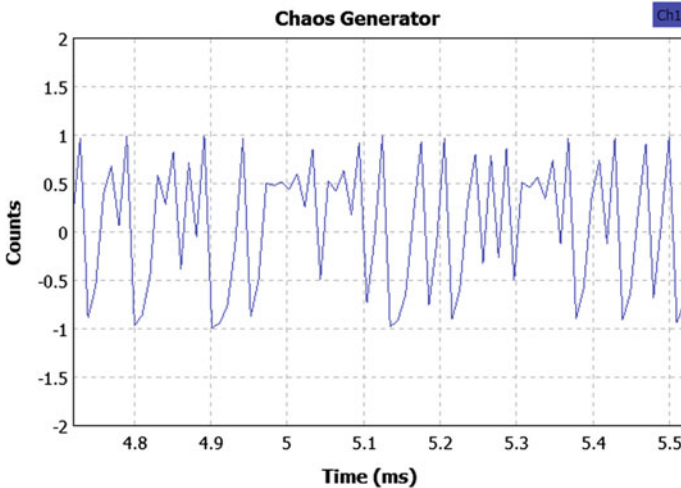


Fig. 3 The output of the Chaotic generator

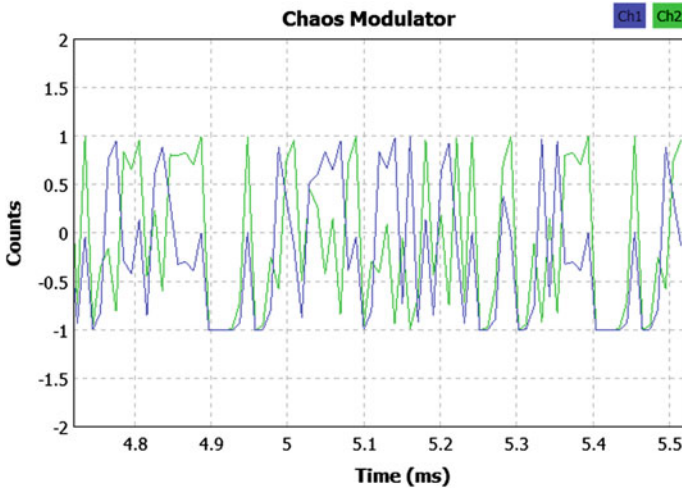


Fig. 4 The output of Chaos Modulator

delayed copies of the received signal. Due to the good auto-correlation properties of the chaotic signal, any symbol misalignment (delay) will result in a very low correlation value between the reference and the data. In order to control the computational complexity and efficiency that this synchronization algorithm required. We set a limiting parameter to the number of delayed copies.

4 Performance Measurement Results of the FM-DCSK System

The analytical BER performance for FM-DCSK system computed under Gaussian approximation [10] is given by:

$$BER = \frac{1}{2} \operatorname{erfc} \left(\sqrt{\frac{E_b}{4N_0} \left(1 + \frac{2 E_b}{5M N_0} + \frac{MN_0}{2E_b} \right)^{-1}} \right) \tag{5}$$

where erfc is the complementary error function, $N_0/2$ is the noise variance, E_b is the bit energy computed at the output of chaotic modulator.

Figure 5 shows measured BER and theoretical BER.

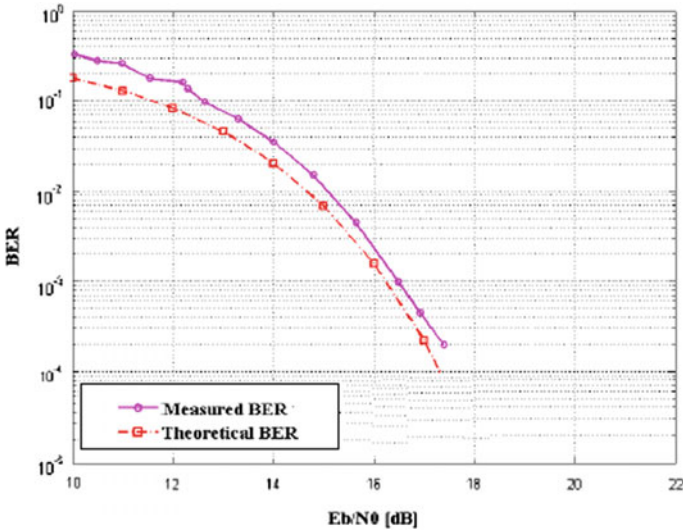


Fig. 5 BER performance of the FM-DCSK system

5 Conclusion

The article describes the implement of a real-time FM-DCSK communication system based on GNU Radio platform, introduces a simple and robust implementation method of chaotic signal generator and symbol synchronization algorithm. System implementation method is suitable for the study and development of the wireless communication system that have a customized requirements about the communication protocol standards and the whole system. It helps to reduce iterative process at a later stage of system development, shorten the development period of the system.

References

1. Hikmat N. Abdullah, Alejandro A. Valenzuela · Performance Evaluation of FM-COOK Chaotic Communication System Journal of Signal and Information Processing 01/2011; 2 (03):175–177. DOI:10.4236/jsip.2011.23023.
2. G. Kaddoum and F. Gagonen, “Error Correction Codes for Secure Chaos-Based Communication System,” *25th Bi-ennial Symposium on Communication*, Kingston, 12–14 May 2010, pp. 193–196.
3. G. Kaddoum, P. Chargé, and D. Roviras, “A generalized methodology for bit-error-rate prediction in correlation-based communication schemes using chaos,” *Comm. Letters.*, vol. 13, no. 8, pp. 567–569, 2009.

4. M. Sushchik, L. S. Tsimring, and A. R. Volkovskii, "Performance analysis of correlation-based communication schemes utilizing chaos," *IEEE Trans. Circuits and Systems*, vol. 47, pp. 1684–1691, 2000.
5. Y. Xia, C. K. Tse, and F. C. M. Lau, "Performance of differential chaosshift-keying digital communication systems over a multipath fading channel with delay spread," *IEEE Trans. Circuits Syst. II, Express Briefs*, vol. 51, pp. 680–684, 2004.
6. Y. Zhang, X. Shen and Y. Ding "Design and Performance Analysis of an FM-QCSK Chaotic Communication System," *2nd International Conference on Wireless Communications, Networking and Mobile Computing*, wuhan, 22–24 september 2006, pp. 1–4.
7. F. C. M. Lau and C. K. Tse, *Z Chaos-Based Digital Communication Systems*. Springer-Verlag, 2003.
8. X. Li, X. Lin, and D. Guo, "The experimental blind timing acquisition scheme for fm-dcsk communication system," in *Anti-Counterfeiting Security and Identification in Communication (ASID)*, 2010 International Conference on, July 2010, pp. 120–125.
9. "GNU Radio." [Online]. Available: <http://gnuradio.org/>.
10. M. A. B. Faran, A. Kachouri and M. Samet, "Design of Secure Digital Communication Systems Using DCSK Chaotic Modulation," *DTIS 2006 International Conference on Design and Test of Integrated Systems in Nano-scale Technology*, Tunis, 5–7 September 2006, pp. 200–204.